

WHAT IS CLAIMED IS:

1. A method of transmitting contents information, comprising the steps of:

- 5 generating a signal representative of a key from authenticator-value information and key base information, the authenticator-value information representing a specified authenticator value, the key base information containing identification information which is set to reproduce the specified authenticator value according to a
- 10 predetermined degeneration function;
- encrypting contents information into encryption-resultant contents information in response to the key signal; and
- transmitting the key base information and the encryption-resultant contents information.

15

2. A method of recording contents information, comprising the steps of:

- generating a signal representative of a key from authenticator-value information and key base information, the authenticator-value
- 20 information representing a specified authenticator value, the key base information containing identification information which is set to reproduce the specified authenticator value according to a predetermined degeneration function;
- encrypting contents information into encryption-resultant
- 25 contents information in response to the key signal; and
- recording the key base information and the encryption-

resultant contents information.

3. A method of transmitting contents information, comprising the steps of:

- 5 generating a signal representative of a key from authenticator-value information and key base information, the authenticator-value information representing a specified authenticator value, the key base information containing identification information which is set to reproduce the specified authenticator value according to a
10 predetermined degeneration function;
encrypting at least the identification information in the key base information to convert the key base information into encryption-resultant key base information;
encrypting contents information into encryption-resultant
15 contents information in response to the key signal; and
transmitting the encryption-resultant key base information and the encryption-resultant contents information.

4. A method of recording contents information, comprising the
20 steps of:

- generating a signal representative of a key from authenticator-value information and key base information, the authenticator-value information representing a specified authenticator value, the key base information containing identification information which is set to reproduce the specified authenticator value according to a
25 predetermined degeneration function;

09726434-120100

encrypting at least the identification information in the key base information to convert the key base information into encryption-resultant key base information;

- 5 encrypting contents information into encryption-resultant contents information in response to the key signal; and
 recording the encryption-resultant key base information and the encryption-resultant contents information.

5. An apparatus for transmitting contents information,
10 comprising:

 means for generating a signal representative of a key from authenticator-value information and key base information, the authenticator-value information representing a specified authenticator value, the key base information containing
15 identification information which is set to reproduce the specified authenticator value according to a predetermined degeneration function;

 means for encrypting at least the identification information in the key base information to convert the key base information into
20 encryption-resultant key base information;

 means for encrypting contents information into encryption-resultant contents information in response to the key signal; and

 means for transmitting the encryption-resultant key base information and the encryption-resultant contents information.
25

6. An apparatus for recording contents information, comprising:

09725434-120100

means for generating a signal representative of a key from authenticator-value information and key base information, the authenticator-value information representing a specified authenticator value, the key base information containing

5 identification information which is set to reproduce the specified authenticator value according to a predetermined degeneration function;

means for encrypting at least the identification information in the key base information to convert the key base information into

10 encryption-resultant key base information;

means for encrypting contents information into encryption-resultant contents information in response to the key signal; and

means for recording the encryption-resultant key base information and the encryption-resultant contents information.

15

7. A transmission medium for transmitting encryption-resultant key base information and encryption-resultant contents information, wherein the encryption-resultant key base information and the encryption-resultant contents information are generated by the

20 steps of generating a signal representative of a key from authenticator-value information and key base information, the authenticator-value information representing a specified authenticator value, the key base information containing identification information which is set to reproduce the specified

25 authenticator value according to a predetermined degeneration function; encrypting at least the identification information in the

key base information to convert the key base information into encryption-resultant key base information; and encrypting contents information into encryption-resultant contents information in response to the key signal.

5

8. A recording medium loaded with encryption-resultant key base information and encryption-resultant contents information, wherein the encryption-resultant key base information and the encryption-resultant contents information are generated by the steps of generating a signal representative of a key from authenticator-value information and key base information, the authenticator-value information representing a specified authenticator value, the key base information containing identification information which is set to reproduce the specified authenticator value according to a predetermined degeneration function; encrypting at least the identification information in the key base information to convert the key base information into encryption-resultant key base information; and encrypting contents information into encryption-resultant contents information in response to the key signal.

10

15

20

9. A method as recited in claim 3, wherein the identification information in the key base information contains at least one of 1) information about a region or regions corresponding to one or more countries, one or more zones, or one or more spaces, 2) information about identification of an individual, 3) information about

25

09726434.120100

- identification of a group of persons, 4) information about a rating, 5) information about identification of an apparatus maker or a device maker, 6) information about identification of a contents provider, 7) information about time, 8) information about contents authors, 9) information about identification of a reproducing apparatus or a reproducing device, 10) information about identification of a connection apparatus or a connection device, 11) information about identification of a medium on which contents information is recorded, 12) information about identification of contents information, and 13) information about accounting.

10. A method of transmitting contents information, comprising the steps of:

- generating a signal representative of a key from key base information containing identification information which is set to reproduce a specified authenticator value according to a predetermined degeneration function;

- encrypting contents information into encryption-resultant contents information in response to the key signal; and transmitting the key base information and the encryption-resultant contents information.

11. A method of recording contents information, comprising the steps of:

- generating a signal representative of a key from key base information containing identification information which is set to

reproduce a specified authenticator value according to a predetermined degeneration function;

encrypting contents information into encryption-resultant contents information in response to the key signal; and

5 recording the key base information and the encryption-resultant contents information.

12. A method of transmitting contents information, comprising the steps of:

10 generating a signal representative of a key from key base information containing identification information which is set to reproduce a specified authenticator value according to a predetermined degeneration function;

encrypting at least the identification information in the key
15 base information to convert the key base information into encryption-resultant key base information;

encrypting contents information into encryption-resultant contents information in response to the key signal; and

transmitting the encryption-resultant key base information
20 and the encryption-resultant contents information.

13. A method of recording contents information, comprising the steps of:

generating a signal representative of a key from key base
25 information containing identification information which is set to reproduce a specified authenticator value according to a

09725434-120300

predetermined degeneration function;

encrypting at least the identification information in the key
base information to convert the key base information into
encryption-resultant key base information;

5 encrypting contents information into encryption-resultant
contents information in response to the key signal; and

recording the encryption-resultant key base information and
the encryption-resultant contents information.

10 14. An apparatus for transmitting contents information,
comprising:

means for generating a signal representative of a key from key
base information containing identification information which is set
to reproduce a specified authenticator value according to a

15 predetermined degeneration function;

means for encrypting at least the identification information in
the key base information to convert the key base information into
encryption-resultant key base information;

20 means for encrypting contents information into encryption-
resultant contents information in response to the key signal; and

means for transmitting the encryption-resultant key base
information and the encryption-resultant contents information.

15. An apparatus for recording contents information, comprising:

25 means for generating a signal representative of a key from key
base information containing identification information which is set

09726434.120100

to reproduce a specified authenticator value according to a predetermined degeneration function;

means for encrypting at least the identification information in the key base information to convert the key base information into

5 encryption-resultant key base information;

means for encrypting contents information into encryption-resultant contents information in response to the key signal; and

means for recording the encryption-resultant key base information and the encryption-resultant contents information.

10

16. A transmission medium for transmitting encryption-resultant key base information and encryption-resultant contents information, wherein the encryption-resultant key base information and the encryption-resultant contents information are generated by the

15 steps of generating a signal representative of a key from key base information containing identification information which is set to reproduce a specified authenticator value according to a predetermined degeneration function; encrypting at least the identification information in the key base information to convert the
20 key base information into encryption-resultant key base information; and encrypting contents information into encryption-resultant contents information in response to the key signal.

17. A recording medium loaded with encryption-resultant key
25 base information and encryption-resultant contents information, wherein the encryption-resultant key base information and the

09726434-120100

encryption-resultant contents information are generated by the steps of generating a signal representative of a key from key base information containing identification information which is set to reproduce a specified authenticator value according to a

- 5 predetermined degeneration function; encrypting at least the identification information in the key base information to convert the key base information into encryption-resultant key base information; and encrypting contents information into encryption-resultant contents information in response to the key signal.

10

18. A method as recited in claim 12, wherein the identification information in the key base information contains at least one of 1) information about a region or regions corresponding to one or more countries, one or more zones, or one or more spaces, 2) information

15

about identification of an individual, 3) information about identification of a group of persons, 4) information about a rating, 5) information about identification of an apparatus maker or a device maker, 6) information about identification of a contents provider, 7) information about time, 8) information about contents authors, 9)

20

information about identification of a reproducing apparatus or a reproducing device, 10) information about identification of a connection apparatus or a connection device, 11) information about identification of a medium on which contents information is recorded, 12) information about identification of contents

25

information, and 13) information about accounting.

00726434.120100

19. A method of decrypting encryption-resultant contents
information generated by an encrypting side which implements the
steps of generating a signal representative of a key from
authenticator-value information and key base information, the
5 authenticator-value information representing a specified
authenticator value, the key base information containing
identification information which is set to reproduce the specified
authenticator value according to a predetermined degeneration
function; and encrypting contents information into encryption-
10 resultant contents information in response to the key signal; the
method comprising the steps of:

reproducing the authenticator-value information
representative of the specified authenticator value from the
identification information in the key base information according to
15 the predetermined degeneration function;

reproducing the key signal from the reproduced
authenticator-value information and the key base information; and
decrypting the encryption-resultant contents information into
the original contents information in response to the reproduced key
20 signal.

20. A method of decrypting encryption-resultant contents
information generated by an encrypting side which implements the
steps of generating a signal representative of a key from
25 authenticator-value information and key base information, the
authenticator-value information representing a specified

09726434-120100

authenticator value, the key base information containing identification information which is set to reproduce the specified authenticator value according to a predetermined degeneration function; encrypting at least the identification information in the

- 5 key base information to convert the key base information into encryption-resultant key base information; and encrypting contents information into encryption-resultant contents information in response to the key signal; the method comprising the steps of:

- decrypting the encryption-resultant key base information into
10 the original key base information;

reproducing the authenticator-value information representative of the specified authenticator value from the identification information in the original key base information according to the predetermined degeneration function;

- 15 reproducing the key signal from the reproduced authenticator-value information and the original key base information; and

- decrypting the encryption-resultant contents information into the original contents information in response to the reproduced key
20 signal.

21. An apparatus for decrypting encryption-resultant contents information generated by an encrypting side which implements the steps of generating a signal representative of a key from
25 authenticator-value information and key base information, the authenticator-value information representing a specified

authenticator value, the key base information containing identification information which is set to reproduce the specified authenticator value according to a predetermined degeneration

- 5 key base information to convert the key base information into encryption-resultant key base information; and encrypting contents information into encryption-resultant contents information in response to the key signal; the apparatus comprising:

means for decrypting the encryption-resultant key base
10 information into the original key base information;

means for reproducing the authenticator-value information representative of the specified authenticator value from the identification information in the original key base information according to the predetermined degeneration function;

- 15 means for reproducing the key signal from the reproduced authenticator-value information and the original key base information; and

means for decrypting the encryption-resultant contents information into the original contents information in response to
20 the reproduced key signal.

22. A method of decrypting encryption-resultant contents information generated by an encrypting side which implements the steps of generating a signal representative of a key from key base
25 information containing identification information which is set to reproduce a specified authenticator value according to a

09726434-120100

predetermined degeneration function; and encrypting contents information into encryption-resultant contents information in response to the key signal; the method comprising the steps of:

- reproducing the authenticator-value information
- 5 representative of the specified authenticator value from the identification information in the key base information according to the predetermined degeneration function;
- reproducing the key signal from the key base information;
- deciding whether or not the reproduced authenticator-value
- 10 information is correct;
- decrypting the encryption-resultant contents information in response to the reproduced key signal when it is decided that the reproduced authenticator-value information is correct; and
- altering the reproduced key signal into a wrong key signal and
- 15 decrypting the encryption-resultant contents information in response to the wrong key signal when it is decided that the reproduced authenticator-value information is not correct.

23. A method of decrypting encryption-resultant contents
- 20 information generated by an encrypting side which implements the steps of generating a signal representative of a key from key base information containing identification information which is set to reproduce a specified authenticator value according to a predetermined degeneration function; encrypting at least the
 - 25 identification information in the key base information to convert the key base information into encryption-resultant key base information;

09725424-120300

and encrypting contents information into encryption-resultant contents information in response to the key signal; the method comprising the steps of:

- 5 decrypting the encryption-resultant key base information into the original key base information;

 reproducing the authenticator-value information representative of the specified authenticator value from the identification information in the original key base information according to the predetermined degeneration function;

- 10 reproducing the key signal from the original key base information;

 deciding whether or not the reproduced authenticator-value information is correct;

- 15 decrypting the encryption-resultant contents information in response to the reproduced key signal when it is decided that the reproduced authenticator-value information is correct; and

- altering the reproduced key signal into a wrong key signal and decrypting the encryption-resultant contents information in response to the wrong key signal when it is decided that the
20 reproduced authenticator-value information is not correct.

24. An apparatus for decrypting encryption-resultant contents information generated by an encrypting side which implements the steps of generating a signal representative of a key from key base
25 information containing identification information which is set to reproduce a specified authenticator value according to a

09726434-120100

predetermined degeneration function; encrypting at least the identification information in the key base information to convert the key base information into encryption-resultant key base information; and encrypting contents information into encryption-resultant contents information in response to the key signal; the apparatus comprising:

means for decrypting the encryption-resultant key base information into the original key base information;

means for reproducing the authenticator-value information representative of the specified authenticator value from the identification information in the original key base information according to the predetermined degeneration function;

means for reproducing the key signal from the original key base information;

means for deciding whether or not the reproduced authenticator-value information is correct;

means for decrypting the encryption-resultant contents information in response to the reproduced key signal when it is decided that the reproduced authenticator-value information is correct; and

means for altering the reproduced key signal into a wrong key signal and decrypting the encryption-resultant contents information in response to the wrong key signal when it is decided that the reproduced authenticator-value information is not correct.

25. A method of decrypting encryption-resultant contents

09726434-120100

information generated by an encrypting side which implements the steps of generating a signal representative of a key from key base information containing identification information which is set to reproduce a specified authenticator value according to a

- 5 predetermined degeneration function; and encrypting contents information into encryption-resultant contents information in response to the key signal; the method comprising the steps of:

reproducing the authenticator-value information representative of the specified authenticator value from the

- 10 identification information in the key base information according to the predetermined degeneration function;

reproducing the key signal from the key base information;

deciding whether or not the reproduced authenticator-value information is correct;

- 15 decrypting the encryption-resultant contents information in response to the reproduced key signal when it is decided that the reproduced authenticator-value information is correct; and

failing to decrypt the encryption-resultant contents information in response to the reproduced key signal when it is

- 20 decided that the reproduced authenticator-value information is not correct.

26. A method of decrypting encryption-resultant contents information generated by an encrypting side which implements the steps of generating a signal representative of a key from key base information containing identification information which is set to

09726434-120100

reproduce a specified authenticator value according to a predetermined degeneration function; encrypting at least the identification information in the key base information to convert the key base information into encryption-resultant key base information; 5 and encrypting contents information into encryption-resultant contents information in response to the key signal; the method comprising the steps of:

decrypting the encryption-resultant key base information into the original key base information;

10 reproducing the authenticator-value information representative of the specified authenticator value from the identification information in the original key base information according to the predetermined degeneration function;

reproducing the key signal from the original key base 15 information;

deciding whether or not the reproduced authenticator-value information is correct;

decrypting the encryption-resultant contents information in response to the reproduced key signal when it is decided that the 20 reproduced authenticator-value information is correct; and

failing to decrypt the encryption-resultant contents information in response to the reproduced key signal when it is decided that the reproduced authenticator-value information is not correct.

25

27. An apparatus for decrypting encryption-resultant contents

09726434-120100

information generated by an encrypting side which implements the steps of generating a signal representative of a key from key base information containing identification information which is set to reproduce a specified authenticator value according to a

- 5 predetermined degeneration function; encrypting at least the identification information in the key base information to convert the key base information into encryption-resultant key base information; and encrypting contents information into encryption-resultant contents information in response to the key signal; the apparatus
- 10 comprising:

means for decrypting the encryption-resultant key base information into the original key base information;

means for reproducing the authenticator-value information representative of the specified authenticator value from the

- 15 identification information in the original key base information according to the predetermined degeneration function;

means for reproducing the key signal from the original key base information;

- 20 means for deciding whether or not the reproduced authenticator-value information is correct;

means for decrypting the encryption-resultant contents information in response to the reproduced key signal when it is decided that the reproduced authenticator-value information is correct; and

- 25 means for failing to decrypt the encryption-resultant contents information in response to the reproduced key signal when it is

09726434.120100

decided that the reproduced authenticator-value information is not correct.

28. A method as recited in claim 19, wherein the identification
- 5 information in the key base information contains at least one of 1) information about a region or regions corresponding to one or more countries, one or more zones, or one or more spaces, 2) information about identification of an individual, 3) information about identification of a group of persons, 4) information about a rating, 5)
- 10 information about identification of an apparatus maker or a device maker, 6) information about identification of a contents provider, 7) information about time, 8) information about contents authors, 9) information about identification of a reproducing apparatus or a reproducing device, 10) information about identification of a
- 15 connection apparatus or a connection device, 11) information about identification of a medium on which contents information is recorded, 12) information about identification of contents information, and 13) information about accounting.

09726434-120100